Theory of Experiential Career Exploration Technology (TECET): Increasing cybersecurity career interest through playable case studies

Justin Scott Giboney
Brigham Young University
justin_giboney@byu.edu

Derek L Hansen
Brigham Young University
dlhansen@byu.edu

Tanner Johnson Brigham Young University
tannerwj@gmail.com

Desiree Winters Brigham Young University
winters.desiree@gmail.com

Jason K McDonald Brigham Young University jason@byu.edu

Jonathan Balzotti Brigham Young University jonathan_balzotti@byu.edu

Elizabeth Bonsignore University of Maryland ebonsign@umd.edu

Abstract

There is a large demand to fill cybersecurity jobs. To alleviate this need, it is important to generate interest in cybersecurity as a career. One way to do this is through job shadowing and internships. Using design science principles, we have built and tested a playable case study (PCS) where participants can act out a virtual internship and learn relevant cybersecurity skills. We ran a study with students in introductory university courses where they played through a simulated internship at a penetration testing company called CyberMatics. In the study we showed that a PCS format helps students 1) better understand what skills and traits are needed for, 2) more firmly decide whether to pursue, and 3) increase their confidence in their ability to succeed in a career in cybersecurity. Through this study we propose the Theory of Experiential Career Exploration Technology (TECET).

1. Introduction

An estimated 1.8 million cybersecurity positions will be unfilled by 2022 [8], and an increasing number of other technical jobs demand cybersecurity knowledge [26]. Despite high salaries and opportunities, there is a lack of awareness of cybersecurity education and job opportunities among millennials who are choosing college majors and careers [2,48]. Attracting female students into the cybersecurity field is particularly challenging, due to current recruitment techniques that focus on abstract puzzle-solving competitions rather than introducing students to what cybersecurity jobs actually entail.

The majority of high school students never hear about cybersecurity as a career option from teachers, mentors, or career counsellors [39] though that number has improved in recent years. Even fewer report an understanding of the nature of the job tasks of cybersecurity professionals [39]. This is unfortunate, as occupational plans in high school are the strongest predictor of student's declared college majors [32]. Retaining students once they have declared a major is also a challenge for Science, Technology, Engineering, and Mathematics (STEM) majors, where over half of all declared STEM majors do not graduate in a STEM field [16]. Research suggests that interventions that build confidence (i.e., self-efficacy), use active learning, and help students identify as a STEM professional are needed to increase persistence in STEM majors [16].

Research specific to girls and cybersecurity is newer and less robust [9,43], but consistent with that for other STEM majors including computer science. Given perceptions by girls that computer-related jobs are primarily limited to programming and gaming [18,43], it is unlikely that many have considered cybersecurity jobs. Industry professionals identify misperceptions about the nature of cybersecurity work and skills [30] and in many cases a lack of knowledge that cybersecurity jobs even exist [43]. Female cybersecurity professionals feel that anyone with the right skills, knowledge, and experience can work in cybersecurity and see it as a highly interesting, challenging, and exciting career, although they worry that women are not recruited, valued, or promoted as much as men [36]. Early work with cybersecurity camps for girls indicates that cybersecurity, as separate from computer science, is likely to be particularly appealing to girls. Specifically, the highly collaborative, creative (i.e., creative problem-solving), real-world and pro-social focus (e.g., hacking; catching bad guys), and communication skills (e.g., secret messages) are highly appealing, as are sub-areas such as forensics, crisis management, and collaborative teamwork (e.g., project management) [24,46]. This is consistent with findings that suggest that women are increasing their footprint in cyber-related fields related

URI: https://hdl.handle.net/10125/59928
ISBN: 978-0-9981331-2-6

to governance, risk, and compliance management, which emphasize skills often associated with women [2]. Topics such as penetration testing that integrate investigative skills with communication, teamwork, compliance, and ethics seem particularly likely to appeal to women.

A number of strategies have been used to help attract and retain more cybersecurity professionals. Unfortunately, many are difficult to scale, not authentic to the actual work of cybersecurity professionals, or are problematic in attracting female students. The most prevalent approach has been the use of cybersecurity competitions which do seem to attract a certain type of student due to their highly engaging nature. However, cybersecurity competitions are expensive and difficult to implement, are offered infrequently, can discourage non-competitive participants (particularly female students), are better suited for measuring skill than developing skills, can lower self-efficacy for those who don't come in with strong knowledge already, can fail to address realistic scenarios, are not calibrated to individual students' needs, and are difficult to integrate into formal classrooms [11,25,31]. They are best suited for reinforcing the interests of those already with high levels of cybersecurity skills, not teaching concepts or recruiting those who don't already know they want to go into cybersecurity [47]. Other approaches like cybersecurity camps [40] and awareness days, have helped spread the word about cybersecurity as a career, but are also not sufficient. They are necessarily short experiences designed for those who already have interests in cybersecurity and can afford them. They also take considerable funding and resources to run, including development of hands-on learning experiences, finding instructors with expertise, travel, and the logistics of food and lodging.

In summary, experiential learning experiences are needed that help students, particularly female students, increase their likelihood of majoring in a cybersecurity discipline and getting a cybersecurity job. They should be designed for freshman or sophomore students who are still choosing a major. They should help students: (a) understand the cybersecurity job, including a deep understanding of the tasks, processes, communication, and mindsets of cybersecurity professionals, (b) develop and apply the knowledge, skills, and abilities in a way that will build their confidence (self-efficacy), (c) utilize active learning strategies, (d) and help them identify as a cybersecurity professional. They should also be easy for instructors to implement in a classroom, low-cost, appeal to a wide variety of students, and fit within a variety of introductory computing courses.

Following a design science research philosophy, we built a simulation called a playable case study (PCS) focused on the work of a cybersecurity penetration tester. Penetration testers are ethical hackers hired by organizations to test and report on vulnerabilities and risks to the organization. One contribution of the paper is to describe this CyberMatics PCS to help inspire future designs. Another is to address the broader research questions:

1) How can a PCS help students: a) better understand what skills and traits are needed for cybersecurity professionals, b) increase confidence in their ability to succeed in a cybersecurity career, and c) increase their desire to pursue a career in cybersecurity?

2) How does a PCS affect males and females differently?

2. Literature review

2.1 Cybersecurity education research

There are many articles related to cybersecurity curriculum development [7,31,38,41,49]. There are also many articles related to cybersecurity awareness or training [1,12,13,23,33]. However, there are few articles that describe methods for generating interest in a career in cybersecurity. Tobey, Pusey, and Burley [47] state that cybersecurity competitions are useful for attracting experienced individuals that will go on to careers in cybersecurity. Bashir, Wee, Memon, and Guo [4] show evidence that those who have higher self-efficacy, a rational decision-making style, and are investigative are more likely to express interest in a career in cybersecurity when competing in competitions. Rowland, Podhradsky, and Plucker [40] describe structures of cybersecurity girls camps designed to increase career interest. Hoffman, Burley, and Toregas [22] provide a holistic view of how to increase the cybersecurity workforce by defining its structure, providing continuous development, and developing educational initiatives. This research builds on existing initiatives by introducing a specific scenario that can introduce college freshman to a career in cybersecurity.

2.2 Playable case studies

Playable Case Studies (PCSs) are interactive simulations that allow students to "play" through an authentic scenario as a member of a professional team [20]. A PCS is a hybrid learning experience that includes an immersive, simulated online environment, as well as accompanying in-class activities and lessons facilitated by a teacher to provide educational scaffolding and metacognition. They are "playable" because students are full participants in an unfolding fictional story. They are "case studies" because they

occur in an authentic, holistic environment designed to pose real-world problems and reflection, which are facilitated by teachers during class time and built-in assessments. They are novel in their use of mixed-reality techniques [5] that allow the fictional story to bleed into players' real life, as they interact with fictional characters via video-conferencing, email, texting, file sharing, multimedia environments, and special-purpose tools used by professionals.

PCSs are a type of experiential simulation [17] and epistemic game [42] designed to help players better understand and make connections between the skills, knowledge, identity, dispositions, values, and epistemology unique to a profession. Like "virtual internships" [10], they allow players to take on the role of a professional before they have the expertise to do so in a professional setting. The technology, narrative, and social experiences embedded in PCSs are inspired by educational Alternate Reality Games, which adhere to the "This is Not a Game" (TINAG) ethos, ideal for creating authentic and engaging mixed-reality experiences [5]. Rather than controlling a virtual avatar, players play as themselves in a "first person" narrative, helping to connect their real identity to the professional identity they are taking on. Though PCSs use elements and inspiration from these other types of simulations, the combination of elements is unique enough to warrant a new genre.

3. CyberMatics Design

In this section we introduce the CyberMatics PCS using a design science research approach. Design science research is a methodology for identifying features of technology to build grounded theories about its operation, optimization, and/or outcomes from a technological and/or behavioral perspective [21,34,35,37]. Design science as a codified research methodology, consists of six steps: 1) identify and motivate the problem, 2) define the objectives of a solution, 3) design and develop an IT artifact, 4) demonstrate the use of the artifact, 5) evaluate the potential value of the artifact, and 6) communicate the design and significance of the artifact and findings [37]. We have already discussed the problem in the introduction. In this section we explain the solution objectives and artifact design that was created. Following sections report on an evaluation that demonstrates the use of the artifact and its potential and significance. We have published details on our iterative design process, design tensions, and rationale for our specific approach elsewhere [ANONYMIZED]. Here we present a detailed description of the CyberMatics PCS and an evaluation of its impact on students.

3.1 Solution objectives

The first objective of CyberMatics is to help students better understand what knowledge, skills, and traits are needed for cybersecurity professionals. Students that better understand the job will be able to better decide whether a career in cybersecurity is right for them.

The second objective is to help fill the large demand for cybersecurity professionals who are likely to enjoy and be proficient at the job. Therefore, we hope the CyberMatics PCS will encourage students to pursue a career in cybersecurity, as well as encourage inclined students to more firmly commit.

Lastly, the third objective is to help students increase their confidence in their ability to succeed in a career in cybersecurity. Hopefully, an increase in their confidence will encourage students to pursue a career in cybersecurity if they have sufficient desire.

3.2 Artifact design and demonstration

CyberMatics is a PCS that is meant to give students a day-in-the-life, simulated experience of a professional penetration tester. Students become employees in a cybersecurity company called CyberMatics right before the company starts a penetration test for a fictional home automation company called Riptech. The player learns cybersecurity terminology and completes tasks (such as SQL injection and password cracking) with the help of pre-created virtual team members. Soon after the penetration test begins, the security team finds out that a rogue member of the home automation company has entered backdoor code into the Riptech system in order to obtain access to customer data. After contacting the Riptech CEO, the CyberMatics team agrees to try to find out who entered the backdoor code. The player does some virtual sleuthing on the RipTech Linux server with the aid of virtual team members, finds out which RipTech employee entered the backdoor code, and records evidence. The simulation ends with a video of the RipTech employee being arrested and a final penetration testing report submitted by the player.

This narrative unfolds throughout 5 simulated days, each of which must be completed in order to advance to the next (see Table 1). Assignments, cybersecurity tools, and educational scaffolding are integrated into the online simulation and supplemented by in-class discussions and lesson plans. The project manager, Sarah, assigns tasks for each of the simulation days (see left-hand side of Figure 1). Once completed, students click the "Move on to next Day" button, which triggers the release of new content for that day including new tasks, group chat messages, video conference calls, documents, etc.

Figure 1. CyberMatics chat interface

Table 1. Simulation days

Day	Narrative	Goals
1	Introduce the team, the scope, the target company–RipTech, and the RipTech CEO.	Students learn the concept of ethical penetration testing and how to navigate the simulation.
2	Visit RipTech.io website. Receive instructions for and start the penetration test. A coworker gets in trouble for violating scope.	Learn about SQL injection and technical report writing. Obtain usernames and password hashes using SQL injection.
3	Look at evidence of a bad actor gathered by a coworker who social engineers his way into the RipTech offices. Use a password to further penetrate the company.	Learn how to crack password hashes in a shell environment.
4	Explore the target company server using remote access. Find more evidence of a backdoor from the bad actor and report it to the CEO who contacts the FBI.	SSH into the target company. Learn more about Linux. Find evidence of bad actor on server files.
5	End the simulation. FBI arrests the bad actor. Write up your sections of the penetration testing report.	Learn how to write up a penetration testing report.

Students interact with other CyberMatics' team members who share their own findings, share advice, and model positive behaviors and negative behavior, which is identified as negative behavior by the project manager and dealt with appropriately. Communication occurs through a realistic, yet simplified interface modeled after a corporate intranet. It includes a group chat system similar to Slack, that uses a chat-bot to dynamically respond to player input from different fictional characters. The system also supports videos, which are presented as conference calls or video feeds uploaded from other characters (Figure 1).

Cybersecurity tools and aids are accessible via the CyberMatics intranet as well. The Terminal interface, a custom simulated shell, allows students to run Linux commands to perform various tasks (Figure 2). Educational scaffolding is incorporated through character chat messages, video-conferencing, and CyberMatics internal documentation on topics relevant to the simulation (Figure 3). In addition, students are meant to cover topics in class such as databases (e.g., SQL) and a high-level security overview before they complete the simulation. Players also add sections to the final penetration testing report (Figure 4) throughout the experience, in order to help reflect on what was accomplished each day from a client perspective. The goal of the interface is to be as authentic as possible, while also simplifying things and allowing students to easily track their progress. All material, including an introduction on how to use the intranet are presented in an "in game" manner consistent with the principle of TINAG described earlier. For example, the introductory video is not from an educator introducing the simulation, it is from a human resources CyberMatics employee welcoming you to the company and showing you around.

Finally, the players perform a penetration test on the Riptech website, which looks like an authentic internet of things company website (Figure 5).

In summary, the PCS online interface has four main features that enhance realism and learning:

1. Predefined task panel and day tracking
2. Simulated interaction with coworkers (Chat)
3. Educational documentation (Docs)
4. Simulated tools (e.g., Terminal and Report sections; Riptech.io website)

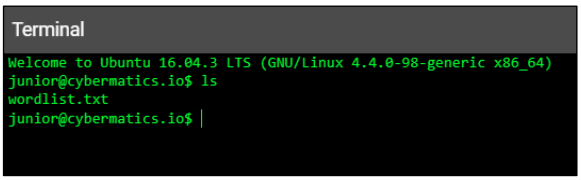

Figure 2. CyberMatics simulated terminal

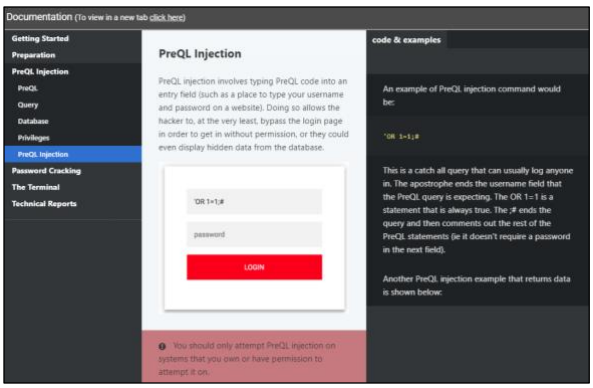

Figure 3. CyberMatics internal docs

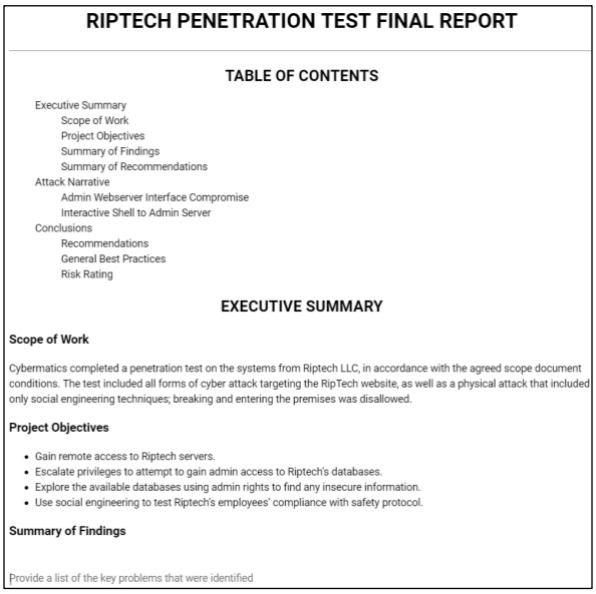

Figure 4. CyberMatics interactive report

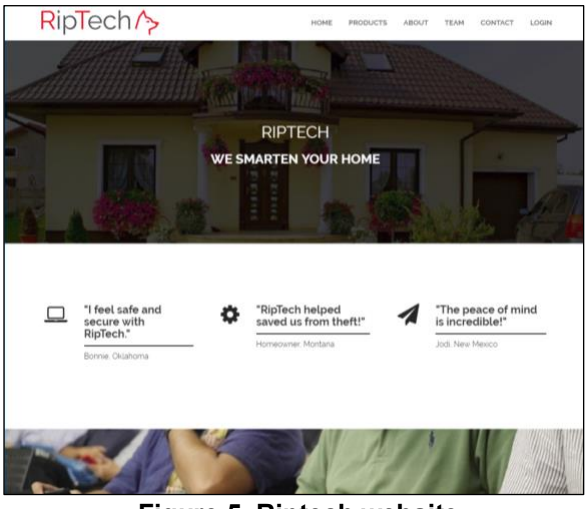

Figure 5. Riptech website

4. Evaluation Methodology

We evaluated the PCS by having 107 students from introductory courses from two universities in different parts of the United States interact with the PCS. 31 students did not complete the interaction or failed attention checks in the survey. This left us with 76 students. 50 (65.8%) of the students identified their sex as male and 26 (34.2%) identified their sex as female. The average age of the 72 students was 20.17 with a standard deviation of 3.18. One class was an introductory information technology (IT) class, primarily consisting of IT majors, though it also included students from ancillary majors exploring IT as a potential. Many of these students have an interest in cybersecurity, which is a major emphasis area within the IT program. The other class was an undergraduate introduction to information science course for students in, or exploring, the major of information science. Fewer of these students focus on cybersecurity, though it is a topic of interest to some. Both teachers were using the CyberMatics PCS for the first time and not part of the design team, though a TA and members of the design team were available to help in the IT class. We would expect that additional refinement of the simulation itself (e.g., improved docs, use of in-class lesson plans) and more experience teaching with the simulation would improve the student outcomes, but the reported results are a good baseline.

We asked a series of questions before and after the interaction. After IRB statements, in the presurvey we measured the students' interest in cybersecurity using a sliding bar from 0 to 100 related to agreement with the following statements: I am interested in cybersecurity, I plan on pursuing a career in cybersecurity, and I feel confident in my ability to succeed in the cybersecurity field. We also measured the student's perception of the importance of various skills to cybersecurity professionals and in separate questions the student's confidence in their own abilities related to the same skills: leadership, communication, adaptability, problem solving, ethics, programming, ability to learn on their own, and attention to detail. We asked the same questions in the post survey so that we could see the effect of the PCS on their responses. In the post survey, we also asked 7-point Likert scale questions about how the PCS changed their view of a career in cybersecurity: The simulation made me more likely to pursue a career in cybersecurity, the simulation made me more confident in my ability to succeed in a cybersecurity career, I would recommend the simulation to people deciding whether to pursue a career in cybersecurity. Qualitative questions included: how have your perceptions about cybersecurity changed after completing the simulation, and if you are not interested

in cybersecurity, please list 3-5 reasons why you are not interested. Other questions focused on what students liked and disliked about the design of the simulation, though they are reported on in another publication focused specifically on the design of the PCS and student reactions to it [ANONYMIZED].

We performed two types of analyses. For questions measured in both the pre- and post-surveys we first ran a paired T-test to look for effects of the PCS. Second, we ran a Welch's T-test of the difference between the post-survey and the pre-survey based upon sex. For questions that only were asked in the pre-survey (e.g., likelihood of recommending the simulation to others), we also evaluated differences in results by gender.

Responses to the two qualitative questions analyzed using a thematic analysis process wherein we iteratively identified key themes that emerged from the data itself. They are primarily used to supplement the quantitative findings.

5. Evaluation Results

Figure 6 shows the self-reported impact of the simulation on students; 34% of students agreed at some level that they were more likely to pursue a career in cybersecurity after the simulation, with males being significantly more likely (Table 2), 45% of students agreed at some level that they were more likely to succeed in a cybersecurity career as a result of the simulation, and 62% of students agreed at some level that they would recommend the simulation to others trying to decide on a career in cybersecurity. While there is room for improvement, these values suggest that the CyberMatics PCS is fulfilling its intended purpose for at least a large segment of students.

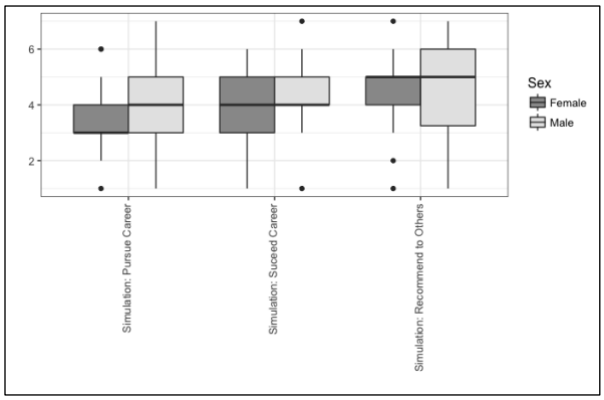

Figure 6. Boxplots of postsurvey questions

Responses between the first 2 questions were highly correlated (r = .55), suggesting that the increase (decrease) in likelihood to pursue a career in cybersecurity may be driven, at least in part, by the increase (decrease) in confidence in the ability to succeed.

Table 2 reports differences between the pre- and post-surveys for each individual, with Figure 7 showing the corresponding box plots. Overall, there was a significant increase in students' confidence in their ability to succeed in a cybersecurity career, with female students showing higher improvement though not significant. Students' understanding of what penetration testers do increased dramatically, suggesting that they had little understanding of the role of penetration testers and their day-to-day activities. Students' recognized the importance of communication as part of the requisite skills needed by cybersecurity professionals more after the simulation. This is likely due to the prominent place that chat messages, video conferences, and the final penetration report took in the simulation. Interestingly, students saw the skill of "attention to detail" as being less important after the simulation, for no reason that is obvious to the authors. Students' confidence in their ability to be ethical also went down after the simulation. This may be because the simulation helped them realize some of the nuances of ethical behavior, such as staying in scope of a penetration test. Students' confidence in their programming skills increased after the simulation. This is likely due to their work with performing database injections and developing their Linux skills. While there were not statistically significant differences between males and females for most questions, this is likely due to the relatively small numbers of female students.

Table 2. Statistical results

Question (difference of 100-point scales)	Pre/Post difference (positive is higher postsurvey)	Sex difference of pre/post differences (positive is higher female)
Interest in cybersecurity	-3.27†	-0.79
Interest in a cybersecurity career	0.41	-6.00
Confidence in ability to succeed in career in cybersecurity	5.55*	6.56
Understanding what penetration testers do	46.65***	2.12
Skills: Leadership	4.35†	3.81
Skills: Communication	4.81*	3.64
Skills: Adaptability	-1.00	-0.76
Skills: Problem Solving	-0.96	-2.28
Skills: Ethics	-0.05	-7.98
Skills: Programming	1.64	-1.86

Table 3. Statistical results continued

Skills: Learn on your own	3.21†	2.67
Skills: Attention to detail	-3.05*	-1.26
Confidence: Leadership	1.57	5.30
Confidence: Communication	-0.60	4.98
Confidence: Adaptability	0.12	1.99
Confidence: Problem Solving	-0.21	-0.73
Confidence: Ethics	-5.20**	-1.70
Confidence: Programming	5.52**	7.08†
Confidence: Ability to learn	2.96†	-2.40
Confidence: Attention to detail	-2.72	-3.50
Simulation made me more likely to pursue a career in cybersecurity		-0.60*
Simulation made me more confident to succeed in a career in cybersecurity		-0.40
I would recommend the simulation to help decide career		0.02

† p <= 0.1, * p <= 0.05, ** p <= 0.01, *** p <= 0.001

When asked how the simulation changed their perceptions of cybersecurity, seven students said that cybersecurity was more complex than they thought. Six students said that cybersecurity was easier than they thought. This is likely due to the different initial perceptions of the field that students hold. Twenty students said that they became more knowledgeable about cybersecurity. Nine students said they were more interested, while two said they were dissuaded because of the simulation.

When asked why they were not interested in cybersecurity, a variety of reasons were given. Fourteen students dislike programming. Six students said they just weren't skilled enough, while one said s/he were too far behind. Four students said it would be too stressful, while one said it would be too risky. Three students said it was not creative enough. Two students said they didn't have enough patience, it was too complex, too time consuming, or wanted more human interaction (each). One student said there was too much writing, too much outside the box thinking, too much effort, too hard to keep up on tools and hacks, hates cubicles, too frustrating, too much math, too much competition, bad problem solver, s/he has the wrong mindset, and too much controlled substance screening (each).

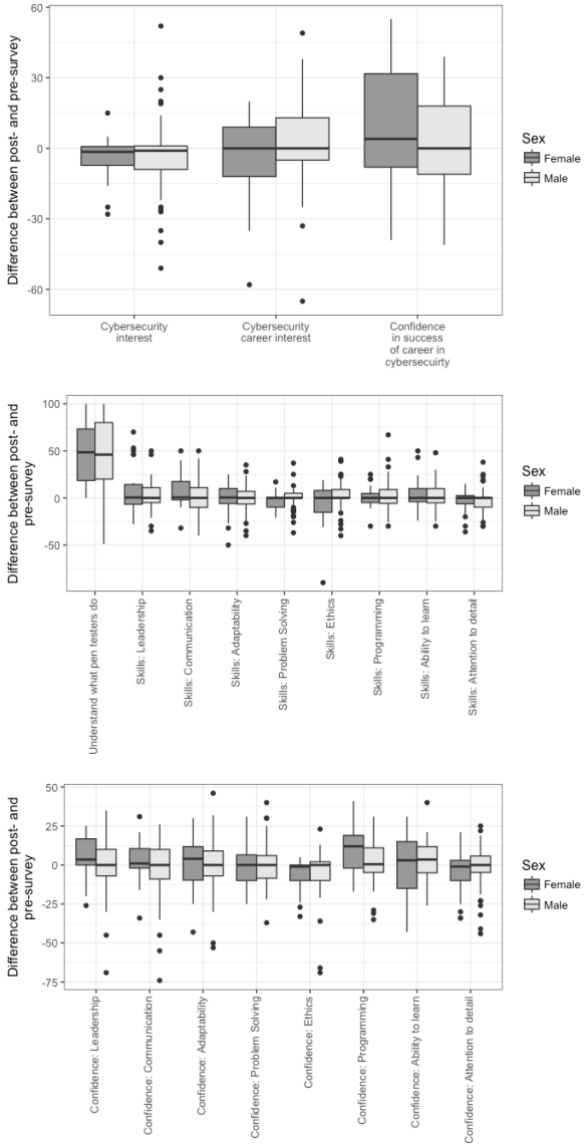

Figure 7. Boxplots of response differences

6. Discussion

Design science research should ultimately lead to theoretical contributions, as well as actionable insights [34]. We hope that the description of our CyberMatics PCS will help inspire additional simulations that use some of the key design ideas and features outlined earlier in the description of CyberMatics. While a full explanation of the features most liked by students and the design choices made by the team is beyond the scope of this paper, the results presented here suggest that the

finalized artifact shows promise as a tool for helping students explore a potential career in cybersecurity at an early stage in their undergraduate education. Particularly given that it was still a beta version of the PCS and taught by instructors who had not taught using a PCS before.

We are currently working hard to update the PCS to reflect specific student comments that identified challenges, such as unclear CyberMatics "docs," mediocre video production quality, and a lack of a more robust chat system. The high correlation between improved confidence from the simulation and likelihood to go into a cybersecurity career suggests how important it is to scaffold the experience in a way that students can succeed; while also recognizing that some students will benefit from learning that they are not sufficiently interested or skilled in the area to want to pursue it. Future studies with larger samples and more diverse student populations will help articulate the full potential of a PCS on student career exploration and choice.

The process of designing an experiential career exploration PCS has given us an opportunity to consider how to build experiential career exploration simulations that will lead to desired student outcomes and behaviors. Based on the results of the simulation we would like to propose the Theory of Experiential Career Exploration Technology (TECET) (See Figure 8). While the elements of this theory are familiar to those who study career exploration, here we emphasize the need to explicitly design technologies to support the various outcomes of interest. Below is a description of each of those outcomes.

P1. ECET use increases decision resolve to pursue a career or not.

First, technology is often used to enhance decision-making [6,14,44,45]. Decision technology can provide a feedback loop where users learn from their mistakes and successes [27]. Research has found that when feedback is incorporated into the decision-making process, decisions become more optimal [27]. Experiential Career Exploration Technology (ECET) provides an opportunity for users to make mistakes and have successes, thus allowing them to make a more informed decision about a future career choice. Additionally, having student take on a specific role during a simulated experience such as the CyberMatics PCS, may help them envision themselves in that role in the future and become more committed to it. Finally, seeing role models like themselves (e.g., a female student who notices a female project manager) may also help students become more resolved to pursue a career.

P2. ECET use increases understanding of the breadth of useful career skills.

Second, students often do not understand or have misconceptions about the skills needed for careers, such as an IT career [19]. Experiential Learning Theory [28,29] states, among other things, that learning is enhanced when material draws out students' beliefs so they can be refined and when there are synergistic transactions between the learner and the environment. When these conditions exist, learners are able to integrate the breadth of a topic into their own understanding [15,28]. ECET provides students an experience that they use to evaluate their own beliefs and integrate into their own understanding. For example, in the CyberMatics PCS students learned that communication skills are critical to cybersecurity work by experiencing multiple communication channels in a realistic setting.

P3. ECET use increase confidence in career skills.

Self-Efficacy Theory [3] states that the more successful attempts a person has of an activity, the more likely that person will feel confident in future attempts. ECET can provide opportunities for users to have successful attempts at skills used in the career. These successful attempts, based on Self-Efficacy Theory will lead to greater confidence in those career skills. By building in educational scaffolding (e.g., CyberMatics docs; chat help) in a realistic scenario, students feel increased confidence not only in their conceptual understanding, but in their ability to apply their skills in a real-world situation.

We note that an increased understanding of the breadth of career skills and confidence in career skills will also indirectly influence the career pursuit decision resolve, though each component should be a separate design goal.

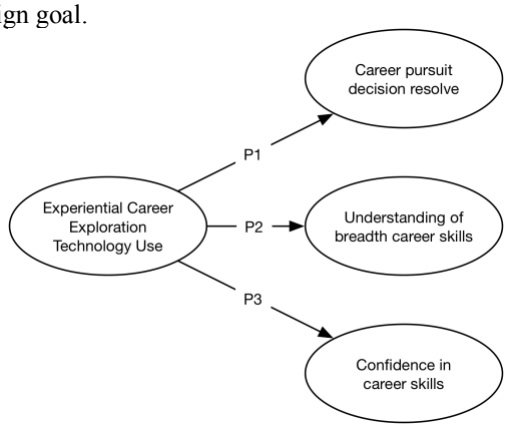

Figure 8. Theory of Experiential Career Exploration Technology

5. Conclusion

With the large demand for cybersecurity candidate it is important to generate interest in cybersecurity as a career. Using design science principles, we built and tested a playable case study (PCS) where participants can act out a virtual internship and learn a diverse set of cybersecurity and professional skills in a complex, unfolding environment. Our description of the CyberMatics PCS is one key contribution of this work. Additionally, our evaluation of students in two introductory university courses showed the promise of such an approach. Through the study we created a theory to help articulate design goals for experiential career exploration technologies, such as PCSs. Specifically, we found that a PCS format helps students 1) better understand what skills and traits are needed for, 2) more firmly decide whether to pursue a career in, and 3) increase their confidence in their ability to succeed in a career in cybersecurity.

6. References

[1] Adams, M. and Makramalla, M. Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review 5*, 1 (2015), 5–14.

[2] Baker, M. Striving for effective cyber workforce development. 2016.

[3] Bandura, A. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review 84*, 2 (1977), 191–215.

[4] Bashir, M., Wee, C., Memon, N., and Guo, B. Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security 65*, (2017), 153–165.

[5] Bonsignore, E., Hansen, D., Pellicone, A., et al. Traversing transmedia together: Co-designing an educational alternate reality game For teens, with teens. *Proceedings of the The 15th International Conference on Interaction Design and Children*, (2016), 11–24.

[6] Burgoon, J.K., Bonito, J.A., Lowry, P.B., et al. Application of Expectancy Violations Theory to communication with and judgments about embodied agents during a decision-making task. *International Journal of Human Computer Studies 91*, (2016).

[7] Bustos, R.A. Facilitating support of cyber: Toward a new liaison model with cybersecurity education at Augusta. *Journal of Business & Finance Librarianship 22*, 1 (2017), 23–31.

[8] Center for Cyber Safety Education, (ISC)2, Booz Allen Hamilton, Alta Associates, and Frost & Sullivan. *2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk*. 2017.

[9] Chai, S., Bagchi-sen, S., Goel, R., Rou, H.R., and Upadhyaya, S. A framework for understanding minority students' cyber security career interests. *Proceedings of the Twelfth Americas Conference on Information Systems*, (2006), 2–7.

[10] Chesler, N.C., Ruis, A.R., Collier, W., Swiecki, Z., Arastoopour, G., and Shaffer, D.W. A novel paradigm for engineering education: Virtual internships with individualized mentoring and assessment of engineering thinking. *Journal of Biomechanical Engineering 137*, 2 (2015), 1–8.

[11] Cheung, R.S., Cohen, J.P., Lo, H.Z., Elia, F., and Carrillo-marquez, V. Effectiveness of cybersecurity competitions. *Proceedings of the International Conference on Security and Management (SAM)*, (2012), 1.

[12] Gavas, E. and Memon, N. Winning cybersecurity one challenge at a time. *IEEE Security & Privacy 10*, 4 (2012), 75–79.

[13] Giannakas, F., Kambourakis, G., and Gritzalis, S. CyberAware: A mobile game-based app for cybersecurity education and awareness. *International Conference on Interactive Mobile Communication Technologies and Learning*, (2015), 54–58.

[14] Giboney, J.S., Brown, S.A., Lowry, P.B., and Nunamaker, J.F. User acceptance of knowledge-based system recommendations: Explanations, arguments, and fit. *Decision Support Systems 72*, (2015).

[15] Godfrey, P.C., Illes, L.M., and Berry, G.R. Creating breadth in business education through service-learning. *Academy of Management Learning & Education 4*, 3 (2005), 309–323.

[16] Graham, M.J., Frederick, J., Byars-Winston, A., Hunter, A.-B., and Handelsman, J. Increasing persistence of college students in STEM. *Science 341*, 6153 (2013), 1455–1456.

[17] Gredler, M.E. Games and simulations and their relationship to learning. In D.H. Jonassen, ed., *Handbook of Research on Educational Communications and Technology*. Mahwah, NJ, 2004, 571–582.

[18] Grover, S., Pea, R., and Cooper, S. Remedying misperceptions of computer science among middle school students. *Proceedings of the 45th ACM technical symposium on Computer science education*, (2014), 343–348.

[19] Gupta, U.G. and Houtz, L.E. High school students' perceptions of information technology skills and careers. *Journal of Industrial Technology 16*, 4 (2000), 1–8.

[20] Hansen, D.L., Balzotti, J., Fine, L., and Ebeling, D. Microcore: A playable case study for improving adolescents' argumentative writing in a workplace context. *Proceedings of the 50th Hawaii International Conference on System Sciences*, (2017), 104–113.

[21] Hevner, A.R., March, S.T., Park, J., and Ram, S. Design science in information systems research. *Mis Quarterly 28*, 1 (2004), 75–105.

[22] Hoffman, L.J., Burley, D.L., and Toregas, C. Holistically building the cybersecurity workforce. *IEEE Security & Privacy 10*, 2 (2012), 33–39.

[23] Jenkins, J.L., Grimes, M., Proudfoot, J.G., and Lowry, P.B. Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development 20*, 2 (2014), 196–213.

[24] Jethwani, M.M., Memon, N., Seo, W., and Richer, A. "I can actually be a super sleuth": Promising practices for engaging adolescent girls in cybersecurity education. *Journal of Educational Computing Research 55*, 1 (2017), 3–25.

[25] Katsantonis, M., Fouliras, P., and Mavridis, I. Conceptual analysis of cyber security education based on live competitions. *Global Engineering Education Conference (EDUCON)*, (2017), 771–779.

[26] Kay, D.J., Pudas, T.J., and Young, B. Preparing the pipeline: The U.S. cyber workforce for the future. *Defense Horizons 72*, August (2012), 1–16.

[27] Kayande, U., De Bruyn, A., Lilien, G.L., Rangaswamy, A., and van Bruggen, G.H. How incorporating feedback mechanisms in a DSS affects DSS evaluations. *Information Systems Research 20*, 4 (2009), 527–546.

[28] Kolb, A.Y. and Kolb, D.A. Learning styles and learning spaces: Enhancing experiential learning in higher education. *Academy of Management Learning & Education 4*, 2 (2014), 193–212.

[29] Kolb, D.A. *Experiential learning: Experience as the source of learning and developmen*. Prentice-Hall, New Jersey, 1984.

[30] LeClair, J. and Pheils, D. *Women in Cybersecurity*. BookBaby, 2016.

[31] McGettrick, A., Cassel, L.N., Dark, M., Hawthorne, E.K., and Impagliazzo, J. Toward curricular guidelines for cybersecurity. *Proceedings of the 45th ACM technical symposium on Computer science education*, (2014), 81–82.

[32] Morgan, S.L., Gelbgiser, D., and Weeden, K.A. Feeding the pipeline: Gender, occupational plans, and college major selection. *Social Science Research 42*, 4 (2013), 989–1005.

[33] Nagarajan, A., Allbeck, J.M., Sood, A., and Janssen, T.L. Exploring game design for cybersecurity training. *IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, (2012), 256–262.

[34] Nunamaker, J.F.J., Twyman, N.W., Giboney, J.S., and Briggs, R.O. Creating high-value real-world impact through systematic programs of research. *MIS Quaterly 41*, 2 (2017), 335–351.

[35] Nunamaker Jr., J.F. and Briggs, R.O. Toward a broader vision for information systems. *Transactions on Management Information Systems 2*, 4 (2011), 20:1-20.

[36] Peacock, D. and Irons, A. Gender inequalities in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology 9*, 1 (2017), 25–44.

[37] Peffers, K., Tuunanen, T., Rothenberger, M.A., and Chatterjee, S. A design science research methodology for Information Systems research. *Journal of Management Information Systems 24*, 3 (2007), 45–77.

[38] Raj, R.K. and Parrish, A. Towards standards in undergraduate cybersecurity education in 2018. *Computer 51*, 2 (2018), 72–75.

[39] Raytheon. *Securing our future: Closing the cybersecurity talent gap*. 2016.

[40] Rowland, P., Podhradsky, A., and Plucker, S. CybHER: A method for empowering, motivating, educating and anchoring girls to a cybersecurity career. *51st Hawaii International Conference on System Sciences*, (2018), 3727–3735.

[41] Shackelford, S.J., Proia, A.A., Martell, B., and Craig, A.N. Toward a global cybersecurity standard of care ?: Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal 50*, 2 (2015), 303–354.

[42] Shaffer, D.W. Epistemic frames for epistemic games. *Computers & Education 46*, 3 (2006), 223–234.

[43] Shumba, R., Ferguson-Boucher, K., Sweedyk, E., et al. Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. *Proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports*, (2013), 1–14.

[44] Speier, C., Vessey, I., and Valacich, J.S. The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance. *Decision Sciences 34*, 4 (2003), 771–798.

[45] Straub, D.W. and Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Quaterly 22*, 4 (1998), 441–469.

[46] Tims, H.E., Turner, G.E., Corbett, K., Deemer, E.D., and Mhire, J. Cyber value and interest development: Assessment of a STEM career intervention for high school students. *Electronic Journal of Science Education 18*, 1 (2014), 1–15.

[47] Tobey, D.H., Pusey, P., and Burley, D.L. Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. *ACM Inroads 5*, 1 (2014), 53–56.

[48] Vogel, R. Closing the cybersecurity skills gap. *Salus Journal 4*, 2 (2016), 32–46.

[49] Yang, S.C. and Wen, B. Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business 92*, 1 (2017), 1–8.